

GeekBrains

Урок 4 Видео 2

Криптография

Hash Length Extension Attack

В этом видео

1. Уязвимая схема MAC-а
2. Особенность схемы Меркла-Дамгора
3. Glue-padding
4. MD padding

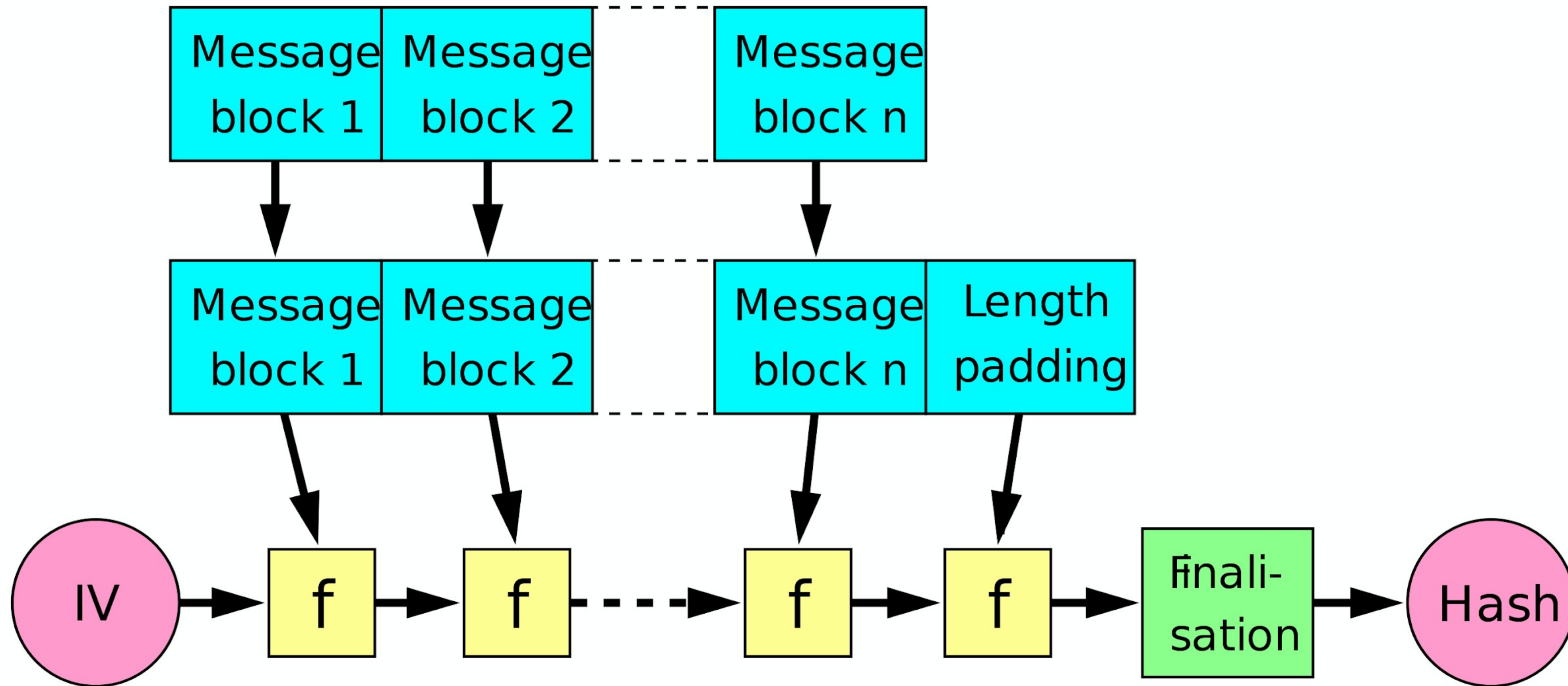
GeekBrains

Уязвимая реализация MAC

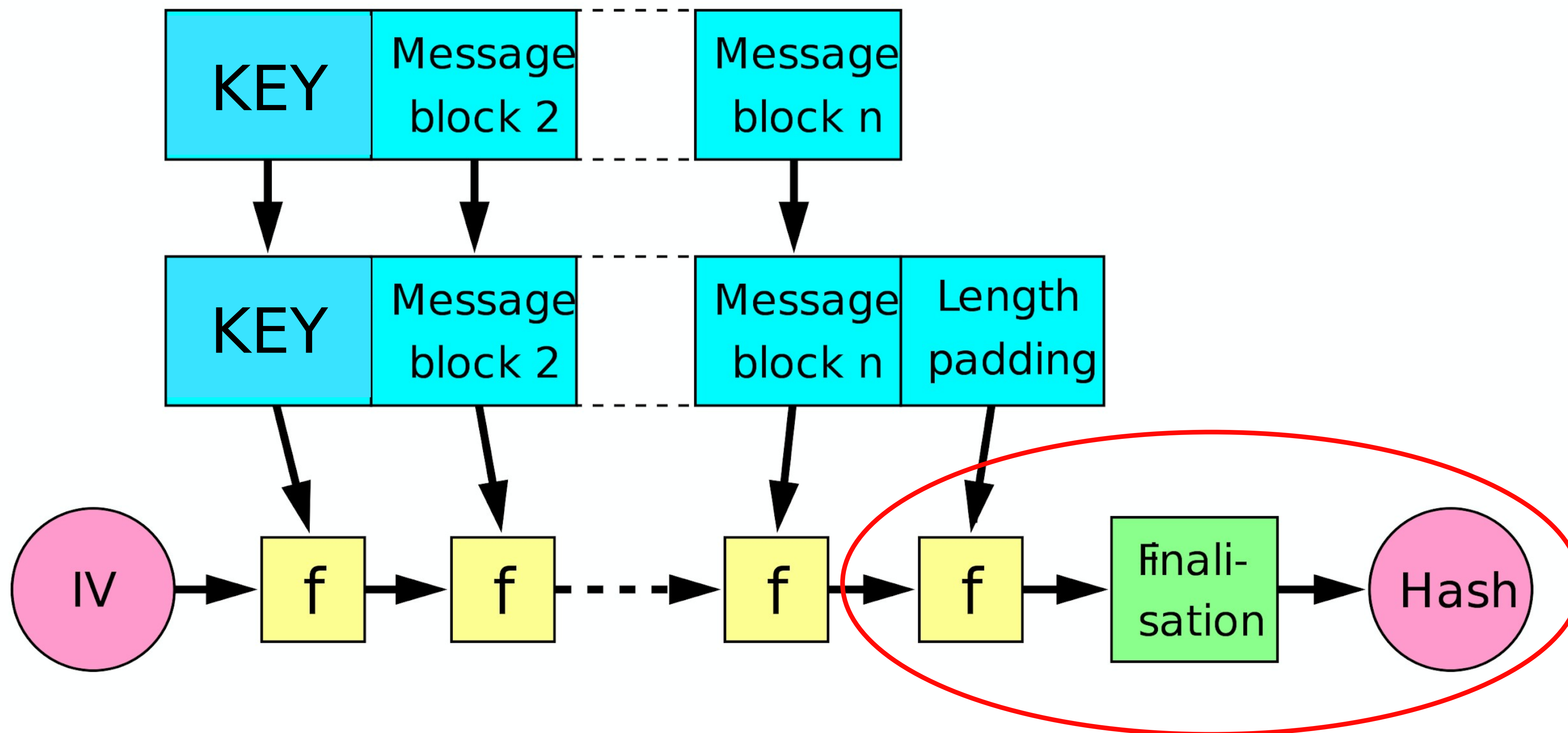
Реализация MAC t = H(k || m) уязвима к Hash Length Extension Attack.



Структура Меркла — Дамгора



Корень проблемы



GeekBrains

Каждый новый блок сообщения меняет внутреннее состояние

Результатом хеширования является внутреннее состояние после обработки последнего блока

67452301EFCDAB8998BADCFE10325476C3D2E1F0



e5fa44f2b31c1fb553b6021e7360d07d5d91ff5e



7448d8798a4380162d4b56f9b452e2f6f9e24e7a



...



a3db5c13ff90a36963278c6a39e4ee3c22e2a436

Заменить IV на MAC исходного сообщения и “дохешировать” произвольные данные (1). Получится MAC для сообщения-подделки.

Дописать glue-padding и произвольные данные в конец сообщения (2). Получится сообщение-подделка.

a3db5c13ff90a36963278c6a39e4ee3c22e2a4
36

↓

9c6b057a2b9d96a4067a749ee3b3b0158d390
cf1

↓

5d9474c0309b7ca09a182d888f73b37a8fe136
2c

↓

...

↓

ccf271b7830882da1791852baeca1737fcbe4b
90

Glue-padding — это паддинг исходного сообщения. Его добавляет сама схема Меркла — Дамгора.

Сообщение-подделка будет выглядеть как:
m || glue-padding || text



MD padding (RFC 3174 - 4)

Добавляем бит “1” в конец сообщения

Заполняем битом “0” все, кроме последних 64 бит последнего блока

В последние 64 бита записывается длина исходного сообщения

Итоги

1. Особенность схемы Меркла-Дамгора
2. Glue-padding
3. MD padding